PGP Universal™ Satellite Version 2.10 for Windows Release Notes

Thank you for using this PGP Corporation product. These Release Notes contain important information regarding this release of PGP Universal Satellite for Windows. PGP Corporation strongly recommends you read this entire document.

PGP Corporation welcomes your comments and suggestions. Please use the information provided in Getting Assistance to contact us.

Product: PGP Universal Satellite for Windows

Version: 2.10.0

Warning: Export of this software may be restricted by the U.S. government.

Note: To view the most recent version of this document, please go to the PGP Support Portal and view the Knowledge Base article *PGP User Guides, Administrator Guides, Quick Start Guides, and Release Notes* (https://support.pgp.com/?faq=589).

What's Included in This File

- About PGP Universal Satellite for Windows
- Changes in This Release
- System Requirements
- Additional Information
- Getting Assistance
- Copyright and Trademarks

About PGP Universal Satellite for Windows

PGP Universal Satellite for Windows automatically encrypts and decrypts email and enforces security policy on all email messages sent to and from the PGP Universal Server. PGP Universal Satellite provides two-way policy enforcement, extending security to inbound email messages originating from outside the organization. It contains virtually no user interface and allows for the centralized management of email security policy.

PGP Universal Satellite for Windows installs on your desktop or laptop computer. It proxies SMTP traffic when you send email messages and it proxies POP and IMAP traffic when you retrieve email messages from your mail server. PGP Universal Satellite for Windows also supports direct MAPI access to Microsoft Exchange Servers and Lotus Notes email client access to Domino servers.

Changes in This Release

This section lists the changes and new features in this release of PGP Universal Satellite for Windows.

What's New in PGP Universal Satellite for Windows Version 2.10

Building on PGP Corporation's proven technology, PGP Universal Satellite for Windows includes numerous improvements and the following new and resolved features:

What's New in Version 2.10

- No changes or new features in this release.

PGP Corporation Compatibility Status with Microsoft Exchange Server 2007

PGP Corporation is pleased to announce compatibility with Microsoft's new Exchange Server 2007. PGP Universal Satellite 2.6 introduced support for Microsoft Exchange Server 2007 and Microsoft Office 2007. When used with Internet-standard PGP/MIME (RFC 3156) messages, full message fidelity is preserved for all secured messages.

With Exchange Server 2007, Microsoft has introduced a change in functionality that converts all messages to its internal MAPI format immediately upon processing, unlike previous versions of Exchange that supported the MIME standard for email. Exchange Server 2007, when both sending and receiving via non-MAPI clients, destroys MIME structures in email. However, PGP/MIME-encoded messages are fully compatible with this Microsoft transition even when MAPI is not in use. All messages sent between PGP Corporation's MAPI clients are also fully compatible.

Please note that messages encoded using the legacy "PGP Partitioned" format may not always display HTML message content properly, and foreign character sets in such messages may not reproduce correctly when processed through Exchange Server 2007. If such messages are processed from non-MAPI clients, the server may delete some encrypted HTML body parts and remove non-ASCII character set information, thus resulting in messages that do not preserve full fidelity. If your organization currently uses the legacy PGP Partitioned encoding with non-MAPI clients, PGP Corporation recommends not upgrading to Exchange Server 2007 at this time. PGP Corporation is working with Microsoft to seek additional solutions for compatibility between Exchange Server and the MIME standard.

PGP Corporation will update the Support Knowledge Base Article #713 (https://support.pgp.com/?faq=713) (as more information becomes available).

System Requirements

- Windows Vista (32- and 64-bit editions), Windows XP (Service Pack 2 or 3), Windows Server 2003 (Service Pack 1), Windows 2000 (Service Pack 4)

  Note: The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

- 512 MB of RAM
- 64 MB hard disk space
- Internet Explorer 6 or greater

Functional Requirements

PGP Universal Satellite requires interaction with a PGP Universal Server. You must be one of the following types of users for PGP Universal Satellite to function:

- A user internal to an organization that has deployed PGP Universal Server. You must have connectivity to the server on port 443 (https) and use one of the supported email clients.
- A user external to an organization's PGP Universal Server. You must have connectivity to the server on port 443 (https).

Compatible Email Client Software

PGP Universal Satellite for Windows will, in many cases, work with Internet-standards-based email clients other than those listed here. PGP Corporation, however, does not support the use of other clients.

PGP Universal Satellite for Windows has been tested with the following email clients:

- Microsoft Outlook 2007 SP1 (Outlook 12)
- Microsoft Outlook 2003 SP3
- Microsoft Outlook XP SP3
- Microsoft Outlook 2000 SP3

- Windows Mail 6.0.6000.16386
- Outlook Express 6
- Mozilla Thunderbird 2.0
- Lotus Notes 6.5.6, 7.0.3, and 8.02
- Novell GroupWise 6.5

Anti-Virus Software Compatibility for Windows

In all anti-virus programs, enabling real-time scanning detects any viruses as the email or attachments are opened. Therefore, although it is recommended to disable email scanning for some of the anti-virus products listed below, your email is still being scanned and you are still being protected by your anti-virus product from viruses spread via email.

Computer Associates eTrust EZ-Antivirus 7.x

- Selective scanning is not compatible with PGP Universal Satellite.

Computer Associates Internet Security Suite 2007

- This product is incompatible with PGP Universal Satellite and should not be installed on the same system as PGP Universal Satellite. [12023]

McAfee Internet Security Suite 2006, McAfee Internet Security Suite 2005, McAfee Internet Security 8.0, McAfee VirusScan 8.x through 10.x

- If email scanning is enabled, the email will not be processed by PGP Universal Satellite. Disable email scanning in the McAfee product and enable real-time scanning.
- No additional special configuration requirements for MAPI email.
- When using McAfee VirusScan Enterprise 8.0i, disable **Prevent mass mailing worms from sending mail** in the **Access Protection Properties** dialog box of the VirusScan console. If this option is enabled, SMTP email will be blocked. To disable this option, right-click the McAfee icon in the System Tray and choose VirusScan Console. Double-click **Access Protection**. In the **Access Protection** dialog box, under **Ports to block**, deselect the box to **Prevent mass mailing worms from sending mail** (this option is enabled by default).

McAfee VirusScan 7.x

- No special configuration required.

Panda Platinum 2005 Internet Security 9.x

- No special configuration required.

Sophos Anti-Virus

- No special configuration required.

Symantec Norton AntiVirus 11.x through 12.x, Symantec Norton Internet Security 2005, Symantec Norton Internet Security 2006

- No special configuration required for MAPI email.
- When using POP email, enable **Auto-Protect** and disable the **Anti-Spam** and **Email Scanning** options. **Auto-Protect**, which is enabled by default, provides protection against viruses in email messages when the message is opened.
- Disable SSL/TLS in Server Settings in PGP Desktop or PGP Universal Satellite. (In PGP Desktop, select the PGP Messaging Control Box and then choose **Messaging > Edit Server Settings**. For **SSL/TLS**, select **Do Not Attempt**. In PGP Universal Satellite, on the **Policies** tab, select **Ignore SSL/TLS**.) These versions of Norton AntiVirus prevent all mail clients from using SSL/TLS, regardless of the use of PGP software.

Symantec Norton AntiVirus 9.x through 10.x, Symantec Norton Internet Security 2003, Symantec Norton Internet Security 2004

- Disable email scanning.

- For Norton Internet Security users, disable **Norton Privacy Control** and **Spam Alert**.
- Disable SSL/TLS in Server Settings in PGP Desktop and PGP Universal Satellite. (In PGP Desktop, select the PGP Messaging Control Box and then choose **Messaging > Edit Server Settings**. For **SSL/TLS**, select **Do Not Attempt**. In PGP Universal Satellite, on the **Policies** tab, select **Ignore SSL/TLS**.) These versions of Norton AntiVirus prevent all mail clients from using SSL/TLS, regardless of the use of PGP software.

Symantec Norton AntiVirus 8.x

- PGP Corporation does not recommend using PGP software with this version of Norton AntiVirus. PGP Corporation recommends that you upgrade to Norton AntiVirus version 10.x or later. [10419]

Trend Micro Antivirus 12.x, Trend Micro PC-cillin Internet Security 2005

- No special configuration required.

Personal Firewall Compatibility

PGP Universal Satellite for Windows has been tested with the following personal firewall software:

- **Zone Alarm:** The Zone Alarm firewall, by default, restricts access to localhost. Because PGP Universal Satellite redirects connections to localhost, this stops PGP Universal Satellite from working correctly. To fix this, add localhost (127.0.0.1) as a trusted IP address in Zone Alarm (on the Firewall/Zones screen). Email proxying by PGP Universal Satellite will work normally once this is accomplished. [6446]
- **CyberArmor Personal Firewall:** PGP Universal Satellite 2.10 is not compatible with InfoExpress CyberArmor Personal Firewall versions 2.6.050802 or 3.2.050802 or prior. Before you install PGP Universal Satellite, you must upgrade these versions: contact your helpline or the vendor (InfoExpress at support@infoexpress.com) for more information. [7010]
- **Webroot Desktop Firewall**: PGP Universal Satellite is compatible with Webroot Desktop Firewall Version 5.8 only. Earlier versions of Webroot software are not compatible with PGP Universal Satellite.

Citrix Compatibility

PGP Universal Satellite for Windows has been tested with the following Citrix software:

- Citrix Presentation Server 4.0
- Citrix Metaframe XP

Additional Information

PGP Desktop

- **PGP Desktop Compatibility**: PGP Desktop includes full support for all PGP Universal Satellite features. PGP Universal Satellite provides a subset of the features of PGP Desktop. If you attempt to install PGP Desktop on a system where PGP Universal Satellite is installed, PGP Desktop overwrites PGP Universal Satellite during installation; also, PGP Universal Satellite will not install over PGP Desktop. Do not install both products on the same system. PGP Desktop version 8.x and earlier users must uninstall PGP Desktop before installing PGP Universal Satellite. [NBN]

Messaging

- **Citrix**: To use PGP Universal Satellite in Citrix environments, download the installer from the PGP Universal Server, *not* through Web Messenger. [17289]
- **POP**: Verizon POP accounts return an incorrect response when connecting to the POPS/SMTPS ports if you have not purchased Verizon's Silver/Gold services. In this situation you must set the ports manually to 110/25 in the Policy user interface for the account, respectively, to avoid connecting to the normal ports. [NBN]
- **RC2 128-bit S/MIME Messages**: PGP Messaging does not support the decryption of RC2 128-bit S/MIME-encrypted email. [12140]

- **Lotus Notes**: When a user has been disabled, email sent by the user is initially blocked. To work around this issue, send the email again and email is sent in the clear, as expected. [12234]
- **Lotus Notes**: When a user has been disabled, and then re-enabled, the user must restart Lotus Notes to send encrypted email. [12236]
- **SMTP**: Activate SMTP AUTH in your email client if it is not currently active. [NBN]
- **S/MIME-signed email messages**: PGP Universal Satellite may not process S/MIME signed emails if the signing X.509 certificate is not included in the email. The certificate is almost always included with the email unless the sender turns off this option. If the message is not processed by PGP Universal Satellite, it may still be processed by the mail client application. [9489, 9491]
- **S/MIME and MAPI**: S/MIME users who intend to use S/MIME with MAPI should ensure that they have an X.509 certificate attached to their keys; otherwise, it is possible that these messages when saved in the Sent Items folder cannot be processed by PGP Universal Satellite. [9858]
- **MAPI/Exchange users and inline objects**: If you are a MAPI/Exchange user, and you are sending messages containing embedded content in a proprietary format (inline objects), PGP Universal Satellite will secure the complete message. This will cause inline objects to be readable/viewable only by recipients in a MAPI/Exchange environment. [5530]
- **Outlook MAPI**: If you are using Outlook in a MAPI environment, use the Messaging Log to confirm the validity of PGP signature annotations in message bodies unless the message was decrypted by your PGP Universal Server, which will do this for you. [6819 + 7304]
- **Outlook 2000 MAPI**: Composing messages while in offline mode when using Outlook 2000 with MAPI is not supported. [8165]
- **Outlook Connector for Notes**: The Outlook Connector for Notes that allows an Outlook client to emulate a Lotus Notes client is not supported. [7567]

Getting Assistance

Documentation and Technical Support

- Online Help is provided as part of PGP Universal Satellite for Windows.
- For more information about using PGP Universal Satellite for Windows, including support, contact your PGP Universal administrator.

Copyright and Trademarks

Copyright © 1991-2009 PGP Corporation. All Rights Reserved. “PGP”, “Pretty Good Privacy”, and the PGP logo are registered trademarks and PGP Universal is a trademark of PGP Corporation in the U.S. and other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.